

Information Technology Oversight Commission (ITOC) Information Technology Policy (ITP) 05-1

Technology Profile: Security / Privacy

Specific Area: Information Technology Security, Incident Response

Purpose: To establish requirements for reporting cyber security incidents

Policy: All *state entities* must report cyber security incidents to the Information Technology Oversight Commission (ITOC) as described in the attached Cyber Security Incident Reporting Procedure. Reporting incidents to a central group promotes collaboration and information sharing with other sites that may be experiencing the same problems. Some of the benefits this provides include the following:

- The ability to coordinate activities among *state entities* experiencing similar incidents to help identify and resolve the problem more quickly than if done separately.
- The ability to coordinate similar *state entities* that may be pursuing legal actions against the intruder.
- The ability to warn and share preventative information to help other *state entities* protect themselves from similar attacks.
- The ability to collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack.

Scope: All state of Indiana governmental bodies connected to the state's backbone to include all branches of government (executive, administrative, legislative and judicial)

Statutory Authority: IC 4-23-16

References: Cyber Security Incident Reporting Policy

Effective Date: August 10, 2004